Application of: Shelton et al.
Serial No.: 10/632,098
Filed: 08/01/2003
Reply to Office Action of 0December 28, 2007

REMARKS/ARGUMENTS

Favorable consideration of this application, in view of the present amendment and following remarks, is respectfully requested.

Claims 1-14 were rejected under 35 U.S.C. § 103(a) over Win et al. (U.S. Patent No. 6,182,142), in view of Bennett (U.S. Patent No. 6,633,587).

The Examiner correctly notes that Win does not disclose either the use of a specific, predefined TCP port number for SNMP commands or the use of SNMP commands at all. In essence, Win is relied on for an intermediary access server 106 that validates a browser 100 before the browser can interact with a downstream protected server 112.

Win itself does not disclose the structure of the amended claims because, to start with, it does not include a switch managed appliance. According to the claims, a switch managed appliance is one that "communicatively couples to the network to couple the workstation to a selected one of plural devices connected to the switch managed device so the workstation can control processing by the selected one of the plural devices." Examples would be KVM switches (*See* claim 15 and specification at pages 1-2) and serial data switches (*See* claim 16 and specification at pages 1-2). The Access Server 106 of Win does not perform that function and thus does not qualify as a switch managed appliance. The difference is important because the present inventions allow a switch device to be directly controlled by SNMP functions after the switch device has done its own authentication. In contrast, in Win, the Access Server is an intermediary device that is authenticating a browser 100 before the browser 100 can obtain access to some other device on the network (such as protected server 112). Win never suggests that the access server is a KVM switch, serial device switch or other switch that can permit a workstation to control processing of an associated selected device.

Application of: Shelton et al.
Serial No.: 10/632,098
Filed: 08/01/2003
Reply to Office Action of 0December 28, 2007

Thus, Win is far afield from the present claims from the start because it isn't addressing SNMP control of *switches*. Secondly, Win doesn't disclose SNMP control of any device of any kind at all. The Office Action, of course, candidly recognizes that fact ("Win fails to explicitly teach a transmission of Simple Network Management Procotol (SNMP) commands" at Office Action page 4). Third, Win does not disclose SNMP control over a predefined TCP port number. So, Win is missing: 1) the basic structure of the present claims, 2) the SNMP control features, 3) the predefined TCP/IP port number, and 4) the correlation between authentication at a switch and the establishment of SNMP control via the predefined TCP/IP port number. The Office Action gives Win too much credit when it says that it "teaches the invention substantially as claimed." For the many missing limitations, the Office Action relies instead on Bennett for the sending of datagram payloads over a connection-oriented link such as TCP/IP.

But, neither Bennett nor Win provides a teaching that makes the necessary link between the login/authentication function and the SNMP switch control over the same TCP port number. Even if, as the office action suggests, Win teaches login/authentication and Bennett teaches SNMP control, the present claims require coordination between the login/authentication function and the SNMP switch control that is present in neither. In particular according to the claims, SNMP control will not occur until the TCP/IP session is properly established on a TCP/IP port number, authenticated on that set TCP/IP port number on the very switch that will be SNMP-controlled on that TCP/IP port number. The session is established over a TCP/IP port number that is the same one used for authentication and then the same one used for SNMP command communication. Bennett teaches a TCP port but it does not explicitly note the value of using that port number, and only that port number, for the follow-up SNMP commands.

And, even if Bennett teaches SNMP control over a common TCP port number, where does it teach that login/authentication occurs over that same TCP port number? It

7
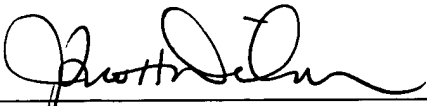
Application of: Shelton et al.
Serial No.: 10/632,098
Filed: 08/01/2003
Reply to Office Action of 0December 28, 2007

doesn't. Of course, Win doesn't teach that either because "Win fails to teach explicitly a predefined Transmission Control Protocl (TCP) port number" (Office action at 3). The common port number used for authentication and SNMP control on the common switch product is not found in the Examiner's combined Win/Bennett hypothetical device. If, for example, Bennett's SNMP function is added to the authentication function of Win, the SNMP function would have to be added to the access server 106 (where the authentication function resides) rather than any qualifying "switch managed appliance." Since the access server 106 does not qualify as the claimed switch, Bennett/Win is SNMP-controlling the wrong thing. If, on the other hand, the Examiner goes still further with the hypothetical and surmises a KVM/Serial switch inserted somewhere into Win where is doesn't explicitly exist, there remains no teaching that that inserted component would have the authentication functions that Win discloses should occur in the *intermediary* device 106 rather than in the ultimate destination device (such as 112). In summary, the combined Win/Bennett hypothetical still does not yield a switch with internal authentication, TCP/IP port-number assigning, and SNMP control over the TCP/IP porting only after authentication on that port number.

An early and favorable allowance is respectfully requested.

	Respectfully submitted,
CUSTOMER NUMBER **42624**	By: _____ J. Scott Davidson Registration No.: 33,489
Davidson Berquist Jackson & Gowdey LLP 4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203 Main: (703) 894-6400 ● FAX: (703) 894-6430	